

REMARKS

This Amendment is filed in response to the Office Action mailed on July 22, 2003. All objections and rejections are respectfully traversed.

Claims 1-128 are in the case.

At paragraph 2 of the Office Action amendment of the specification to replace attorney docket numbers with USPTO serial numbers was required. The specification was accordingly amended.

At paragraphs 3-4 of the Office Action a non statutory double patenting rejection was issued in view of copending Application Number 09/309,045.

Applicant respectfully urges that claim 1 of the present application recites:

1. A method of proving entity membership in a nested group, wherein a presenter of credentials performs the step of *presenting to a recipient of credentials one or more chains of group credentials*.

Applicant respectfully urges that co-pending application does not claim the step of *presenting to a recipient of credentials one or more chains of group credentials*.

That is, the copending application does not claim *chains of group credentials*.

Further, Applicant further urges that the step of *presenting to a recipient of credentials one or more chains of group credentials* is a patentably distinct feature of the present invention which sets the present invention patentably apart from copending Application Number 09/309,045.

Accordingly, Applicant respectfully requests that the Examiner withdraw the double patenting rejection, because of the absence from claims of copending Application Number 09/309,045 of any claim to the step of *presenting to a recipient of credentials one or more chains of group credentials*.

At paragraph 5 of the Office Action Claims 101-128 were rejected under 35 U.S.C. § 101 on the grounds that a “computer data signal embodied in a carrier wave and representing a sequence of instructions” is not patentable subject matter.

Applicant respectfully points out that MPEP 2106 IV, B. 1. (c) (Page 2100-14 of the Eighth Edition) states:

“Natural Phenomena Such as Electricity and Magnetism.

... However, a signal claim directed to a practical application of electromagnetic energy is statutory regardless of its transitory nature."

Applicant respectfully points out that the form of Claims 101-128 meet the "practical application" requirement of MPEP 2106 IV, B, 1 (c) because the claim is to:

101. *A computer data signal embodied in a carrier wave* and representing a sequence of instructions that, when executed by a processor in a network device requesting a service from a server, configures the network device to operate as a client device that:

- A. obtains one or more chains of group credentials to prove client membership in a nested group, and
- B. presents to the server a request for the service, said request including the chains of group credentials.

Further, Applicant respectfully points out that the claimed *A computer data signal embodied in a carrier wave* is a practical use of electromagnetic energy, and is patentable subject matter under 35 U.S.C. § 101, in view of the clarification set out in MPEP 2106 IV, B, 1 (c).

Accordingly, Applicant respectfully urges that Claims 101-128 meet all statutory requirements of 35 U.S.C. § 101, particularly as further set out in MPEP 2106 IV, B, 1 (c).

At paragraphs 6-7 of the Office Action, claims 1-128 were rejected under 35 U.S.C. § 102(b) as being anticipated by Gasser. The U. S. Patent number of Gasser was not given. However, Applicant reviewed the file of copending application Serial No.

09/309,045 and determined that Gasser is most probably U. S. Patent No. 5,220,604 issued June 15, 1993 to Gasser, et al., hereinafter Gasser.

Accordingly, Applicant will argue the rejection in view of Gasser, U. S. Patent No. 5,220,604.

The present invention, as set forth in representative claim 1, comprises in part:

1. A method of proving entity membership in a nested group, wherein a presenter of credentials performs the step of *presenting to a recipient of credentials one or more chains of group credentials*.

Gasser discloses a "global naming service" (hereinafter GNS) which maintains copies of group membership certificates signed by an authority located elsewhere in a "clean" environment. When a client seeks access to a resource, the resource makes an inquiry to the GNS, the GNS searches certificates of authority for that resource, and if the client is found listed on a certificate, then access to the resource is granted.

Applicant respectfully urges that Gasser has no disclosure of Applicant's claimed novel *presenting to a recipient of credentials one or more chains of group credentials*. Further, Applicant respectfully urges that Gasser has no disclosure of *chains of group credentials*.

Chains of group credentials are further described in the present Specification at various pages as:

Page 5, lines 17-26

In accordance with the invention, a presenter of credentials presents to a recipient of credentials one or more chains of group credentials to prove entity membership or non-membership in a nested group in a computer network. The ability to present a chain of credentials is particularly important when a client is attempting the prove membership or non-membership in a nested group and one or more of the group servers in the family tree are off-line. A chain of group credentials includes two or more proofs of group membership and/or proofs of group non-membership. Furthermore, the proofs of group membership may include one or more group membership certificates and/or one or more group membership lists; and proofs of group non-membership may include one or more group non-membership certificates and/or one or more group membership lists.

Page 6 lines 15-- page 7 line 9

The basic concept of the invention is to have a presenter of credentials present to a recipient of credentials one or more chains of group credentials to prove membership or non-membership in a nested group. These chains of group credentials include two or more proofs of group membership and/or group non-membership, such as group certificates and/or group membership lists. The exemplary embodiment is directed to the client-server situation wherein the client is not individually authorized for access to a resource but may gain access by means of a group membership certificate (necessary for access to a particular resource) or a group non-membership certificate (when a group is specifically excluded from access to a resource). These certificates will include time stamps designating the date and time of issue. For each resource that it protects, a resource server typically establishes an expiration period beyond which an issued certificate ceases to be valid.

The presentation of one or more chains of group credentials is not limited to the client-server situation. Any network entity may present credentials, including chains of group credentials, to another network entity. For a given transmission, the entity presenting credentials is defined as a presenter of credentials, and the entity receiving the credentials is defined as a recipient of credentials. A particular entity may be a presenter of credentials in one transmission and a recipient of credentials in a second transmission. For example, Alice and Bob may want to share resources, in which case each would have to present credentials to the other. When Alice transmits credentials to Bob, Alice is a presenter of credentials and Bob is a recipient of credentials. Alternatively, when Bob transmits credentials to Alice, Bob is a presenter of credentials and Alice is a recipient of credentials.

Page 11 lines 1-16

In a different example, the G1 group server may grant membership to anyone who can prove membership in group G11 and non-membership in group G12. Accordingly, Alice will retrieve a group membership certificate from the G11 group server and a group non-membership certificate from the G12 group server and present those certificates to the G1 group server. The G1 group server will then issue a G1 group membership certificate which Alice will present to Bob. If the G1 group server is off-line, Alice will need to present to Bob two chains of credentials, including proofs of group membership and non-membership. Specifically, Alice will need to present to Bob a first chain including a group G1 membership list (signed by G1), along with the group membership certificate from group G11, and a second chain including the signed group G1 membership list, along with the group non-membership certificate from group G12. In this case, because Alice does not need to twice present the signed group G1 membership list, Alice simply presents the signed group G1 membership list, along with the group G11 membership certificate and the group G12 non-membership certificate. Thus, in order to prove membership in a nested group, Alice will sometimes need to present both proofs of group membership and proofs of group non-membership.

Page 12 lines 14 - 24

The case of off-line group servers becomes more difficult when trying to prove non-membership in a nested group. For example, if in the above example the G2, G7, and G8 group servers are off-line, Alice will need to present a chain of credentials to Bob, including proofs of both group membership and group non-membership. Specifi-

cally, Alice may present to Bob a group G2 membership list (signed by G2), a group G7 membership list (signed by G7) and a group G8 membership list (signed by G8). From these credentials, Bob will be aware of the memberships of groups G2, G7 and G8, and Bob will be able to indirectly verify that Alice is not a member of any of these groups. In particular, Bob will know that group G7 lists groups G9 and G10 as members. Therefore, in order to prove non-membership in group G7, Alice will also need to present to Bob group non-membership certificates for the groups G9 and G10.

Page 18 lines 19-29

If at decision block 618 client Alice 104 receives a group membership certificate, client Alice 104 moves back up the family tree, presenting a certificate of membership in each child group to each higher level parent group server at block 620. At block 622 client Alice 104 transmits to resource server Bob 110 the group membership certificate associated with the highest group in the chain, i.e. the root group authorized for access on the resource ACL 114.

At decision block 624 resource server Bob 110 attempts to validate the group certificate presented at block 622. The validity of the group certificate is determined by verifying its signature and by further verifying that its time stamp falls within the recency requirements for the resource. If the validation fails, access is denied at block 604, otherwise access is granted at block 626.

Applicant notes that The Examiner suggested, at paragraph 7 of the Office Action, at page 5 lines 2-5 that Gasser's "subgroups" are the same as Applicant's claimed "chains", in the following passage:

"Members are listed in a certificate (credentials) that which is nested groups that include subgroups (chains) that are certified (proven/validated entity membership) (col. 10 lines 19-55)." (OA, par. 7, p. 5 lines 2-5)

Gasser at Col. 10 lines 19-55 discloses groups, subgroups, and group certificates.

For example, at Col. 10 lines 52 - 65 Gasser states:

“For example, consider a group having as its members the principals P1, P2, P3, . . . pn (where P1 etc. are either individual principals or other subgroups (principal sets). Such a group is represented by a certificated for each principal set . . . These certificates have the same form as the certificates that certify a principal, except that certificates that authenticate a principal associate a particular public key with a principal's name, whereas group certification keys associate a particular principal with a group.”

Accordingly, Gasser discloses only group certificates. Gasser has no disclosure of Applicant's claimed novel *presenting to a recipient of credentials one or more chains of group credentials*. That is, Gasser has no disclosure of *one or more chains of group credentials*.

Therefore, Applicant respectfully urges that Gasser is legally precluded from anticipating the presently claimed invention under 35 U.S.C. § 102 because of the absence from Gasser of any disclosure of Applicant's claimed novel *presenting to a recipient of credentials one or more chains of group credentials*. That is, Gasser is silent concerning *chains of group credentials*.

All independent claims are believed to be in condition for allowance.

All dependent claims are believed to be dependent from allowable independent claims, and therefore in condition for allowance.

Favorable action is respectfully solicited.

Please charge any additional fee occasioned by this paper to our Deposit Account
No. 03-1237.

Respectfully submitted,

A handwritten signature in cursive script, reading "A. Sidney Johnston". The signature is written in dark ink and is positioned above the printed name and address.

A. Sidney Johnston
Reg. No. 29,548
CESARI AND MCKENNA, LLP
88 Black Falcon Avenue
Boston, MA 02210-2414
(617) 951-2500